A COMPREHENSIVE STUDY ON CYBERSECURITY

An essay submitted in partial fulfillment of

the requirements for graduation from the

Honors College at the College of Charleston

with a Bachelor of Science in

Computer Science

KRISTA GROOMS

MAY 2014

Advisor: RoxAnn Stalvey

Krista Grooms

Cybersecurity Bachelor's Essay

Fall 2013

Cybersecurity and Its Modern Day Implications

ABSTRACT

In February 2013, President Barack Obama signed an executive order to discuss how the United States of America should proceed with cybersecurity. This policy acknowledges that cyberspace is widespread and the results of an attack on the digital infrastructure of the United States could be harmful to America and her allies. Months after this order was established, Edward Snowden released top secret documents that disclosed information about the National Security Agency (NSA). These documents made it apparent that the NSA had been collecting large amount of data not only on suspected terrorists, but also on American citizens and her foreign allies. Worldwide discussions of not only the NSA, but cyber threats in general, have since followed. While the United States has stood by the legality of the program, many people have questioned whether or not the program is producing sufficient enough results to merit the infringement upon rights. The question also arises, if it is ethical for the United States to target foreign nationals that they suspect of terrorism or if this infringes upon their personal rights as well. An investigative study was performed that analyzed multiple ways that people are vulnerable to cyber-attack. While the NSA is a large portion of this research information was also discovered about cyber threats that may occur. The results of this study will be used to produce a plan of action that can be applied in everyday life to combat cybersecurity as it pertains to our everyday lives.

BACKGROUND

Beginning the Spring of 2013 I began an intensive research on cybersecurity in hopes that by the end of the 2014 Spring semester I would be able to propose new ways that we not only as computer scientists, but as people in general, can guard ourselves from cyber-attacks. My original research conducted in the Spring of 2013 revolved mostly around case studies done on WikiLeaks, SCDOR Breach, and basic information on the NSA. As I was wrapping up my research, the first information from Edward Snowden was released. While I had already done research on the NSA based off of information given by an employee who worked in the same building as an alleged NSA headquarters, the leaked information from Snowden had a worldwide audience due to Snowden's position within the NSA. The online organization ZDNet described the aftermath of the Snowden leak as the post-Snowden era in which the internet went from

being seen as a global information and communications utility to a utility that is also a "global surveillance machine – for both government and private sectors"[1].

PURPOSE

I believe it is important that I start with just a basic overview as to what Snowden released about the NSA and what this has meant worldwide. After this introduction, I will also list other ways that we are vulnerable to online attacks. This information will be used throughout the Spring of 2014 to construct an artifact that will lay forward a plan of action for combating cybersecurity threats.

SNOWDEN – THE INSIDER THREAT

On June 9, 2013 in a Hong Kong hotel, Edward Snowden leaked top-secret government documents regarding NSA surveillance programs to both *The Guardian* and *The Washington Post*. He currently is living in Russia where he has been granted asylum for one year escaping the international arrest warrant on espionage charges that have been issued by the United States. The documents released to the press included information on how the NSA collects data and what kind of data the NSA has access to. He specifically described the NSA PRISM operations which includes how the United States collects phone call records to search for possible foreign terrorist links and the surveillance of online communications to and from foreign targets that might show suspicious behavior. Snowden had access to all of this information through his job as a Booz Allen Hamilton contractor where he worked as a systems administrator at a NSA Threat Operations Center in Hawaii.[2]

One of the greatest quotes I have found regarding the information leakage by Edward Snowden has come from IBRS security analyst James Turner which states, "The NSA has proven that it can't control its own data internally on its own network, because someone just walked out with classified documentation. So what have other people been walking out with over the years?"[3]

This quote shows what I believe to be one of the greatest issues with the NSA in that while they are collecting all this data that is spread out throughout the internet they are also a central hub for the information. Therefore it would make it easier for a threat to infiltrate the NSA and gain all of this information in one fatal swoop then if the information had to be collected throughout the internet separately. This attack may come from an outside threat or as in Snowden's case the insider threat. Currently people are worried about what other kinds of information Snowden may have to release or even that if he stole information other NSA officials may have also. With the amount of controversy that has followed Snowden's information theft, another incident against the United States may cause more trouble and distrust both within the United States and between the United States and other countries.

---

[1] http://www.zdnet.com/snowdens-legacy-and-the-nsa-of-everything-7000023757/
[2] http://www.boomerangbeat.com/what-is-the-nsa-controversy-and-what-did-edward-snowden-leak/
[3] http://www.zdnet.com/snowdens-legacy-and-the-nsa-of-everything-7000023757/

NATIONAL SECURITY AGENCY

PRISM

An article posted online by *The Washington Post* one week after Snowden's leak to the press about the NSA PRISM program went into detail on all that was known about the program at the time. Following the announcement from Snowden, Director of National Intelligence James Clapper admitted to PRISM's existence and nothing more was mentioned other than it was enacted in 2008 and was governed by Section 702 of the Foreign Intelligence Surveillance Act. [4] According to the classified document that Snowden leaked, the Washington Post stated that, "PRISM enables 'collection directly from the servers' of Microsoft, Yahoo, Google, Facebook and other online companies."[5] While these companies denied that they provided direct access to their servers they did state that they still provide information following FISA requests.[6]

A major point for the PRISM program is that it should only target foreign nationals yet there only has to be 51% chance the person is not a United States Citizen before their information can be tracked.[7] The document released by Snowden showed that in January 2013 the NSA monitored a total of 124.8 billion phone calls. Government watchdog site Cryptome, compiled multiple documents and reports to show that the largest amount of calls originated from Afghanistan and Pakistan with 21.98 billion and 12.76 billion calls monitored respectfully.[8] This same report also found that the United States is able to easily monitor these calls because many international calls run through U.S. carriers as they are cheaper.

RECENT NSA CORPORATE SPYING

In late October 2013, CNET reported on new information that the NSA was tapping directly into Google and Yahoo private fiber-optic networks to access their users' data that is stored in the cloud. The report noted that the NSA works in combination with their British equivalent the Government Communications Headquarters (GCHQ) under a program called MUSCULAR.[9] This program allows the agencies to intercept the companies data within the United States and overseas where unencrypted user data is stored multiple times on different servers.

The NSA responded with the following statement after the news was first reported by the Washington Post.

---

[4] http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/
[5] http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/
[6] http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/
[7] http://www.boomerangbeat.com/what-is-the-nsa-controversy-and-what-did-edward-snowden-leak/
[8] http://news.yahoo.com/nsa-spied-on-124-8-billion-phone-calls-in-just-one-month--watchdog-group-claims-213633988.html
[9] http://news.cnet.com/8301-13578_3-57610061-38/nsa-taps-into-google-yahoo-clouds-can-collect-data-at-will-says-post/

> NSA has multiple authorities that it uses to accomplish its mission, which is centered on defending the nation. The Washington Post's assertion that we use Executive Order 12333 collection to get around the limitations imposed by the Foreign Intelligence Surveillance Act and FAA 702 is not true. The assertion that we collect vast quantities of U.S. persons' data from this type of collection is also not true. NSA applies Attorney General-approved processes to protect the privacy of U.S. persons -- minimizing the likelihood of their information in our targeting, collection, processing, exploitation, retention, and dissemination. NSA is a foreign intelligence agency. And we're focused on discovering and developing intelligence about valid foreign intelligence targets only.[10]

While this statement is meant to confirm that the United States did nothing illegal, it does not clearly state that they did not tap into the private networks to collect information on supposed terrorists. In response to the news that the NSA was intercepting traffic inside Google and Yahoo private networks, Microsoft recently announced that they too would begin encrypting their Internet traffic and data in order to stop NSA spying without the proper requests.[11]

NSA NATIONAL RESPONSE

Following the NSA exposure in early 2013 the United States became split on the NSA. While there are multiple issues supporting and opposing the NSA, proponents of the NSA generally agree that it is necessary the NSA continue if it helps stop terrorist attacks. Opponents of the NSA argue that our freedom of speech is more important than the protection the NSA provides and that if the NSA continues, we are losing the freedom upon which the United States was built. A survey conducted by USA Today in June 2013 revealed that 56% of the polled population said the NSA's tracking of calls to investigate terrorism was acceptable while 41% said this was unacceptable.[12] These close margins show just how much indifference there is on this issue within the U.S.

A separate survey conducted by YouGov and reported by the Washington Post, showed that the majority of the United States citizens polled had no real idea on what the NSA did. Approximately 1/3 of the 1000 people surveyed believed that the NSA listened to the content of calls, captured and killed terrorist and conducted detainee interrogations, when in fact the NSA does none of these things.[13] Poll analyst Amy Zegart stated that the results of the poll also showed that, "Americans will give their government more leeway if they can be convinced counterterrorism tools are effective."[14]

---

[10] http://news.cnet.com/8301-13578_3-57610061-38/nsa-taps-into-google-yahoo-clouds-can-collect-data-at-will-says-post/

[11] http://www.washingtonpost.com/business/2013/11/30/ae61a06a-562c-11e3-8304-caf30787c0a9_story.html

[12] http://www.boomerangbeat.com/what-is-the-nsa-controversy-and-what-did-edward-snowden-leak/

[13] http://www.washingtonpost.com/world/national-security/polls-lesson-for-nsa-show-that-surveillance-programs-actually-combat-terrorism/2013/11/10/1e095442-47ed-11e3-a196-3544a03c2351_story.html

[14] http://www.washingtonpost.com/world/national-security/polls-lesson-for-nsa-show-that-surveillance-programs-actually-combat-terrorism/2013/11/10/1e095442-47ed-11e3-a196-3544a03c2351_story.html

RECENT WORLDWIDE RESPONSE

It is assumed that every county does some level of intelligence gathering. Yet initially following Snowden's release of information about the NSA the world was split on the legality of the NSA. The biggest shock I believe for many people came with knowledge of exactly how much information the NSA was collecting.

In late October 2013 the greatest response I believe thus far came when many of the United States allies called out the Obama administration on the NSA's surveillance of fellow allies. Both Germany and France received information that the NSA had been collecting information on them. German Chancellor, Angela Merkel, called President Obama and the U.S. ambassador complaining about information she received stating the NSA had been spying on her phone calls. She even mentioned that she expected this from other entities, but not from a nation with whom she thought was a strong ally. Upon questioning White House spokesman Jay Carney stated that Obama assured Merkel that, "the United States is not monitoring and will not monitor the communications of the chancellor."[15] This however did not assure that the United States had never monitored her communications. German politician, Wolfgang Bosbach stated, "we are all outraged, across party lines … this cannot be justified from any point of view by the fight against international terrorism or by averting danger."[16]

Along with the German controversy, French newspaper, *Le Monde,* published allegations that the NSA had engaged in mass surveillance of French citizens, including 70.3 million items of French telephone data between December 10, 2012 and January 8, 2013.[17] The citizens targeted included not only people suspected of terrorism but also people in French business and politics. Outraged by this news, French Prime Minister, Jean-Marc Ayrault stated, "President Francois Hollande has asked that the topic be added to the summit agenda. It is not only a French question but a European one … We need to protect ourselves and must demand that new rules are put in place."[18]

Following these allegations the European Union summit in October focused mainly on the NSA allegations brought forth by Germany and France. While the European Union decided not to take any further action against the United States at this point, they did task both Germany and France to find out further information from the United States. While it is not likely that anything will come of this, the EU would have the power to stop the transfer of bank data to the U.S. and could stop agreements on free trade between the United States and Europe.[19] The United States should take this action as a warning and work on a compromise with the EU in regards to the NSA.

---

[15] http://news.msn.com/world/us-ambassador-summoned-by-germany-over-nsa-spying?ocid=ansnews11
[16] http://news.msn.com/world/us-ambassador-summoned-by-germany-over-nsa-spying?ocid=ansnews11
[17] http://news.msn.com/world/france-wants-us-spying-on-europe-summit-agenda
[18] http://news.msn.com/world/france-wants-us-spying-on-europe-summit-agenda
[19] http://www.wsws.org/en/articles/2013/10/26/eusu-o26.html

EXPLOIT KITS

On October 15, 2013 I attended an online webinar presented by Phil Owens entitled, ThreatTrack Security VIPREcase **Exploit Kits Exposed**. This webinar began by describing Exploit Kits as a malicious toolset that bets that users won't keep their machines up to date which will grant the malware access to their system. An interesting statistic provided stated that the top seven applications including Adobe and Java had over 1,000 known vulnerabilities last year which represents a 98% increase in the past five years. These are the programs that the exploit kits try to target, because the kit developers know that while most people keep their operating system up to date many 3rd party applications don't stay updated.

This is a dangerous form of cybersecurity threat, because these kits will infect the victims' computer when a compromised web page or malicious link is opened. These websites look like average pages, but once the bug is loaded it holds the infected users system hostage, usually until a fee is paid and will usually result in all information stored on the hard drive to be deleted.

The use of exploit kits is a huge aspect of cybersecurity because they can do a whole lot of damage, require virtually no expertise to implement, and can be bought from as low as $50 a day. The webinar stated that some of the simplest and most effective exploit kits work by clicking on links in malicious spam email and that it is often found in shortened URLs, (think tinyURL). Some of these kits are exhaustive and may even recreate entire emails from websites like CNN or other pages that people usually follow and they will look like their legitimate counterparts. The best way to avoid an exploit kit attack is to never click and follow links, but to always copying and paste or type the URL address directly.

INSIDER THREAT

One of the greatest challenges that can affect cybersecurity is the insider threat. While a company or organization can do things to protect themselves from an outside threat one of the hardest things to do realize is when someone within the organization is going to do it harm. This type of attack is dangerous because the spy usually will have access to everything they need and is aware of the low points in the company that can be used to destroy them. One of the most recent examples of this would be the insider threat the NSA encountered when Snowden released Top Secret information to the public.

The FBI has an online counterintelligence/insider threat document that describes, "the thief who is harder to detect and who could cause the most damage is the insider -- the employee with legitimate access." It is the 'legitimate access' part that makes the insider threat so destructive. When companies hire people they usually go through some sort of screening process and in the case of most government agencies, they are able to acquire different levels of security access. After this process companies assume that the employee is no longer a threat to

them, but either through false information given or changing loyalties they still may become an insider threat. The FBI document mentioned above also states that there are many personal factors which may lead someone to become an insider threat, these include but are not limited to: greed, financial need, anger, adventure, blackmail, ego, compulsive and destructive behavior, and divided loyalty. They go on to mention that these people may be identified by their work habits which may include accessing information that do not need for the scope of their duties, working odd hours without authorization, unreported foreign contacts, unexplained affluence, and concern they are being investigated. An organization may deter insider threats by providing regular training to employees on security and other protocols, protecting sensitive material, monitoring the network for suspicious activity, and providing an easy way for other employees to report suspicious activity.[20]

CONCLUSION

In conclusion through my research I have found that the most destruction caused by cybersecurity is usually caused by the known or unknown human error. As is done with insider threats and exploit kits the targets of these attacks usually never know that they are being attacked until it is too late to stop. These attacks are effective because no one ever wants to believe that what they do may be putting them in danger and therefore usually ignore any signs that something may go wrong. In many cases research both in the Spring and Fall of 2013 there are also technical things that people do that leave them more prone to cyber-attacks. These include but are not limited to not encrypting data and allowing easy access onto systems.

To combat these issues in the future it is going to be important that people know not only what to expect from a cyber-attack, but what they can do to protect themselves beyond the level of protection provided by the system developer.

[20] http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

Works Cited

Dreier, Christoph. "World Socialist Web Site." *NSA Wiretapping Scandal Dominates EU Summit*. N.p., 26 Oct. 2013. Web. 5 Nov. 2013.

"The Insider Threat." *FBI*. FBI, n.d. Web. 2 Dec. 2013.

Lee, Timothy B. "Here's Everything We Know About PRISM to Date." *Washington Post*. The Washington Post, 12 June 2013. Web. 22 Nov. 2013.

"Microsoft Moves to Encrypt Its Internet Traffic." *Washington Post*. The Washington Post, 30 Nov. 2013. Web. 3 Dec. 2013.

Moulson, Geir. "US Ambassador Summoned by Germany over NSA Spying." *MSN News*. MSN, 24 Oct. 2013. Web. 5 Nov. 2013.

Moyer, Edward. "NSA Taps into Google, Yahoo Clouds, Can Collect Data 'at Will,' Says Post." *CNET News*. CBS Interactive, 30 Oct. 2013. Web. 5 Nov. 2013.

Owens, Phil. "Exploit Kits Exposed." Lecture. Threat Track Security VIPREcase Exploit Kits Exposed. Webinar. 15 Oct. 2013. *Threat Track Security*. 15 Oct. 2013. Web. 15 Oct. 2013.

Pfeiffer, Eric. "NSA Spied on 124.8 Billion Phone Calls in Just One Month." *Yahoo! News*. Yahoo!, 23 Oct. 2013. Web. 5 Nov. 2013.

Pincus, Walter. "Poll’s Lesson for NSA: Show That Surveillance Programs Actually Combat Terrorism."*Washington Post*. The Washington Post, 11 Nov. 2013. Web. 20 Nov. 2013.

Reuters. "France Wants US Spying on Europe Summit Agenda." *MSN News*. MSN, 22 Oct. 2013. Web. 5 Nov. 2013.

Stilgherrian. "Snowden's Legacy and the NSA of Everything." *ZDNet*. N.p., 2 Dec. 2013. Web. 2 Dec. 2013.

"What Is the NSA Controversy and What Did Edward Snowden Leak?" *BoomerangBeat*. N.p., 13 June 2013. Web. 15 Sept. 2013.

Krista Grooms

Cybersecurity Bachelor's Essay

Spring 2014

Future Strategy for Cybersecurity

ABSTRACT

President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation". Worldwide, cyber-attacks happen almost constantly. The targets of these attacks include not only individuals, but larger organizations and even countries. I believe by understanding current risks, predicting future risks, and putting safeguards in place we may be able to diminish cybersecurity threats in the future. It is important that we not only teach these strategies to adults, but also to children as they are more accepting of technology which leaves them vulnerable to cyber-attacks. Furthermore, it is a necessity that we begin teaching these techniques to current computer science students who will be able to integrate what they have learned into their future computer programs; in turn leading to the replacement of risky code with programs that can battle cyber-attacks.

BACKGROUND

In the spring of 2013 I began my research into cybersecurity focusing mainly on United States policy towards cybersecurity and real world cyber-attacks. Through this extensive study I found that the majority of all cyber-attacks occur as a combination of program faults and user error. For example, during my research of the 2012 South Carolina Department of Revenue information breach, it was found that the South Carolina Department of Revenue was attacked through direct access into their system by an outside threat. In this case, South Carolina Department of Revenue employees were targeted through a phishing attack in which an email was sent that had a harmful link which allowed the attackers direct access to the network. It only took one South Carolina Department of Revenue employee falling victim to the phishing attack for the network security to be breached. The South Carolina Department of Revenue also contributed to the attacks by not encrypting their data which made it easier for the attackers to use the data.[21] As a conclusion to my research, I came to the conclusion that for us as a generation to protect ourselves from the rising threat of cyber-attacks we must put forth a plan of action that guarantees we are all better aware of the part we must all play in protecting our own cyber data.

21 Shain, Andrew. "State Credentials Used to Access SC Taxpayer Data." The State, Oct. 2012. Web.

PURPOSE

It is important that I lay out that my goal of this document is to suggest an appropriate plan of action that can be implemented to help inform individuals of ways in which they can contribute to cybersecurity. As concluded in my previous essay, I have found that most destruction caused by cybersecurity is usually caused by human error. As is proven with insider threats and exploit kits the targets of these attacks usually never know that they are being attacked until it is too late to stop. These attacks are effective because no one ever wants to believe that they may be putting themselves in danger and therefore usually ignore any signs that something is wrong.

To protect cybersecurity in the future it is going to be important that people know not only what to expect from a cyber-attack, but what they can do to protect themselves. As a solution to this need, I have proposed the following plan of action and published a website with relevant information at https://sites.google.com/a/g.cofc.edu/cyber-security/.

PROPOSAL

Within the past six months, multiple polls have been published naming cyber warfare one of the biggest domestic concerns. A Pew Research Poll found that 70% of the general public believe cyber-attacks from other countries to be a major U.S. threat.[22] Defense News also recently published a poll taken from some of the highest positions among government, civilian, and corporate leaders, 45%, of whom believe cyber warfare to be our greatest threat as a nation.[23] While many government agencies have come out with their plans to tighten cybersecurity I believe that we as individuals should start taking action towards protecting ourselves since we have the greatest amount to lose. I propose to do so, we begin by classifying people into one of four categories, each of which would have best practices in place to teach them about cybersecurity and suggest ways in which they can safeguard their own cybersecurity.

PLAN OF ACTION

As proposed, I believe the best plan of action is to make sure we are aware of cybersecurity risks and are taking preventative actions against cyber-attack. Individually I believe we all fit into one of four categories that can be used to determine the individual plan of actions we should follow.

1. Professional Workforce –These individuals have experience with technology and use it every day both personally and at work.

22 Fryer-Biggs, Zachary. "Leadership Poll." Defense News. Defense News, 5 Jan. 2014. Web.
23 "Public Sees U.S. Power Declining as Support for Global Engagement Slips." Pew Research Center for the People and the Press RSS. Pew Research, 3 Dec. 2013. Web.

2. K – 12 grade –Growing up with technology these children are not as questioning and therefore left vulnerable to attack. This age needs to be informed of the risks and consequences of cyber activity.

3. Retired Workforce – Many of these individuals are new to technology and need to be informed of how their information is being targeted.

4. Computing Community –Through instruction either at the college or professional level, good cybersecurity practices need to be taught so that future software can stand stronger against cyber-attacks.

PROFESSIONAL WORKFORCE

When discussing how and why the current workforce should be educated about cybersecurity, it is important to understand how often they are in contact with technology. Beyond everyday uses such as ATMs and credit card transactions, these individuals are also responsible for the majority of technology systems that are used by businesses. The employees that use these systems can cause an adverse effect on the systems which in turn can harm a countless number of people. For example, when the South Carolina Department of Revenue experienced a data breach in 2012 the attackers gained access through the system by an employee who fallen victim to a phishing attack. The employee clicked a link in an email which allowed the attackers direct access into the SCDOR system. This is a perfect example that illustrates the need for stronger cybersecurity training in the workforce, because if the employee at fault would have received training they may not have fell victim to the attack which would have saved the state upwards of $25 million.[24]

In February of 2013 the United States Government Accountability Office published a report on cybersecurity in which they outlined their findings and recommendations on current cybersecurity practices. The article began by stating that from the period of 2006 to 2012 the rate in which federal agencies had reported cybersecurity incidents to the United States Computer Emergency Readiness Team had increased by 782 percent. The GAO then went further outlining what they considered the main challenge areas that need improvement to slow down this growing trend of cyber-attacks. One of the highlighted areas was the need to promote education, awareness, and workforce planning. A report the GAO published in 2011 stated the main agencies, such as the Department of Homeland Security, responsible for leading the strategic planning efforts for education and awareness had not yet developed details on how they were planning to achieve their outcomes. The 2013 GAO report went a step further in recommending that the federal agencies all needed to take a number of steps to improve agency

[24] Adcox, Seanna. "S.C. Revenue Department Director: Agency Working to Restore Credibility." *The Post and Courier* [Charleston] 23 Apr. 2013. Web.

and government-wide cybersecurity workforce efforts such as developing cyber workforce plans and providing cybersecurity training to their workforce.[25]

Privacy Rights Clearinghouse publishes information on security breaches that have been reported to date as far back as 2005. From January 1 – April 22, 2014 a total of thirty six breaches had been reported that were solely linked to hacking which they define as electronic entry by an outside party, malware, and spyware. While thirty six breaches do not sound that significant many of these breaches attacked hundreds of thousands of people some affecting more than a million individuals. For example a security breach in Neiman Marcus stores left approximately 1.1 million individuals open to attack after their credit card and billing information was stolen. In March of 2014 the City of Detroit also announced a security breach in which the files of approximately 1,700 city employees were stolen after a security breach caused by an employee who clicked on a link that contained malware which froze the files that contained employee names, date of birth, and social security numbers. [26] In both of these situations if the workforce was more informed about cybersecurity, they may have not only been able to prevent the attack, but if the attack still happened, they would have been able to identify the attack had happened and stop it before their customers were infected.

These types of attacks all show the importance of educating the current professional workforce. Many of these attacks happened due to employees clicking on harmful links which downloaded malicious code onto their computers which in turn affect the company's servers. It is important that during employee training, employees are taught what to look for in an email that proves they are legitimate and that they are taught what good URLs look like. Many times the URLs may be shortened or attached to a word. It is important however that the whole URL is examined to make sure it seems credible. In addition, it is also good practice to type the URL into the web browser instead of clicking the link to make sure you are being directed to the correct place. It is also important that the individuals in this group know the proper protocol for reporting a cybersecurity breach. For this item it is important that the leaders in the workforce take action to thwart off attack by making themselves aware of the specific attacks their company is vulnerable too. They can then come up with a plan of action that is specific to their organization that relays what attacks the employees should look for and protect against and what they should do if they suspect a security breach has occurred.

K – 12th GRADE

While discussing issues resulting from cyber-attacks we often find ourselves naming targets such as corporations, governments, and individuals for their information such as credit cards and

[25] "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." *U.S. GAO*. GAO, 14 Feb. 2013. Web.
[26] "Chronology of Data Breaches." *Privacy Rights Clearinghouse*. Web.

passwords to secure sites. Vary rarely do we ever hear someone mention how cyber-attacks can affect children. In reality children are one of the best targets for cyber criminals because their identification links to perfect credit and they most likely won't find out their identity was stolen until they go to apply for credit cards or college loans in their late teens. Children are also more likely to disclose personal information online and share their passwords with people because they do not realize how dangerous the consequences can be, both actions which can lead to cyber stalking, cyber bulling, and even real life predator attacks.

With over 81% of teens using social media, children are almost always susceptible to attacks, especially when they access social media sites on devices like Smartphones which they have constant access to.[27] For example, the most common form of cyber bullying is for the bully to log into the victims social media accounts and then post revealing information that in most cases is not even true.[28] This is dangerous to a child's mental health and stability and can affect multiple aspects of their lives.

Children also tend to over share information on social media which leads to them getting into trouble by making them vulnerable to attacks. For instance, while most adults know not to post that they are heading out of town on vacation, children may post about it which allows thieves to ransack the family home. Also posting information about where they are going to be at each moment and geo-tagging locations in statuses allow child predators to know their locations. Many sites warn of the dangers of geo-tagging photos and then posting them online. For example an article on digitaltrends.com details an incident in which, "September 2010, three men burglarized more than 18 homes in the Nashua area of New Hampshire simply by tracking residents' movements online and, when they were away, broke into their homes and took off with more than $100,000 worth of goods."[29] While in this incident, no one physically was injured if criminals can use geo-tagging to burglarize homes it is not much of a stretch to say they can use it as a way to stalk and attack children.

With the projected need for cybersecurity experts, it is important that children at this age are also aware of current cybersecurity issues and best practices to ensure cybersecurity. In the UK plans, are already in motion to get children as young as eleven training and lessons in the field of cybersecurity. This campaign known as the Secure Futures schools campaign is beginning by teaching teachers how to promote cybersecurity in the classroom so that they can then teach the information to their students. These courses will then continue through the rest of the students' school careers until they transfer to the university level, where university and business partners are going to be given support for promoting cybersecurity. The United Kingdom Universities

[27] Sterling, Greg. "Pew: 94% Of Teenagers Use Facebook, Have 425 Facebook Friends, But Twitter & Instagram Adoption Way Up." *Marketing Land*. 21 May 2013. Web.
[28] "Cyberbullying." *Kentucky.gov*. Office of the Attorney General, 2012. Web.
[29] Schiffner, Bill. "Could You Fall Victim to Crime Simply by Geotagging Location Info to Your Photos." *Digital Trends*. 22 July 2013. Web.

and Science Minister David Willetts stated that "Today countries that can manage cybersecurity risks have a clear competitive advantage" and "By ensuring cybersecurity is integral to education at all ages, we will help equip the UK with the professional and technical skills we need for long-term economic growth."[30] This plan of action if executed correctly may have the desired response to have the United Kingdom leading in cybersecurity efforts in the upcoming future, which as stated by Minister Willetts will give the UK a clear competitive advantage.

For this reason I believe it is important that we as a nation begin to promote cybersecurity activities as well to the younger generation. In additional to formal cybersecurity training in schools which would expose the children to the basics of cybersecurity and the fundamentals of protecting cyber information. I believe it is also important that at an early age, we begin exposing our children to the dangers of cyber-attacks so that they know what to expect and how they can protect themselves. There are many great websites, like connectsafely.org, which give advice to parents on how to talk with their children about internet safety.[31] To ward off personal attacks like cyber bullying it is important to remind children that they need strong passwords that cannot be easily guessed and that they should never share these passwords with anyone. It is also important that children are aware of phony scams on the internet and that not everyone is honest on the internet. It is important to remind children that they should never meet anyone in person or give personal information about themselves to anyone that they have met online no matter who the person says they are or promises to give in return. These people may be trying to abuse or kidnap them and extort their parents for a ransom. Going a step further, it is also important to ensure that children who use social media sites have strong privacy settings turned on that helps protect their information from these would be attackers. Overall, it is important to remind children if they have any questions about something they are doing online that they should stop and ask an adult for advice and help, because most times when something sounds too good to be true it usually is.

RETIRED WORKFORCE

When referring to the retired workforce, we are focusing mainly around the elderly and adults who no longer have or need access to industrial systems. Therefore the technology they are around the most revolves around their personal systems. While this group includes individuals who are very knowledgeable in regards to technology and computer safety, many of these individuals are not. It is important that this age group is aware of the unique attacks, they are vulnerable to and know how to protect themselves from attack.

While researching the ways in which these groups of people are affected by cybersecurity threats, the recurring threat they are vulnerable to is phishing attacks. Phishing attacks are

[30] "School Children as Young as 11 to Get Cybersecurity Lessons." *Gov.uk*. 13 Mar. 2014. Web.
[31] Collier, Anne. "Cybersecurity Where Kids Are Concerned." *Connect Safely*. 1 Oct. 2013. Web.

defined as an online method used by scam artists to steal money and personal information. These attacks often occur in an e-mail masquerading as a message from a trusted source such as a bank or credit card company. They typically ask you to verify your account information immediately with the threat of a negative consequence if you do not comply. The e-mails will also include logos, text, and links to the website which make the e-mail appear legitimate. These correct looking aspects along with the threat of immediate negative consequences trick their victims into providing the requested personal information such as a banking account number, social security numbers, healthcare information, and passwords. [32]

This group of individuals tends to fall victim to phishing attacks more often than younger age categories because they fall for the official looking documents that accompany the emails. They tend to believe they are a good judge of character in real life and assume this skill transfer to online activity. With their life experience, they are usually able to determine the credibility of stores they may walk into, however the technique of judging by looks does not transfer well to the online world where criminals can make very believable cover stories for scams. They also tend to fall for these attacks because they take pride in their good name and when a phishing attacks promises to cause harm if not acted upon quickly they will tend to over share information just to protect their credibility.

The National Council on Aging names Health Care, Medicare, and Health Insurance Fraud as the top scam attack on seniors. [33] This once again shows how vulnerable the retired workforce is because it is very easy for phishing attacks to search for individuals over sixty-five. These attacks can then focus on Medicare related issues. This type of scam is very effective in making the attackers money because they know the individuals in this group rely on Medicare and seeing as it is a government run program, many of them will not question the authenticity of the email. This in turn will lead to the individuals becoming victimized from the phishing attack.

When determining ways in which to educate the retired workforce to protect their cyber safety it is important to remind them of applications that are available to help. For example, by having virus protection and firewall software they can help protect themselves from viruses that may be downloaded if they click on a bad link. At times these viruses may lock their computers and only unlock their computers if payment is made or the virus will threaten to remove all their files. It is also important that they learn how to make secure passwords for websites and they know not to write down these passwords where anyone may be able to gain access to them. These passwords if taken into the wrong hands may lead to stolen identities. In regards to phishing attacks, it is important that this group of individuals knows what to spot in an email that may prove it is a phishing attacks. Key words like Dear Sir or Madame show that the sender does not know who the email is supposed to address, if it is from the actual bank it should

[32] "Threat Terminology." *Network Experts*. Web.
[33] "Top 10 Scams Targeting Seniors." *National Council on Aging*. Web. 2013.

include the recipient's name. If the email promises to take action by tomorrow instead of providing an actual date, this may also show that it is a phishing attack. It is also important to look at the actual email address of the sender of the email. While the contact name may say something along the lines of the bank's name, the email address it is actually being sent from may be something like JoeTheThief@stealyouridentity.com. Overall it is important to remind this age group that respectable companies will never ask for your personal information through email. If they are asking for this information it is better to call the bank or other company directly at their phone number and verify the information with them directly. At this point they will most likely tell you they did not request this information through email and they can report the attack to the appropriate authorities.

COMPUTING COMMUNITY

While the three previously listed groups need to work on ensuring cybersecurity safety today, it is the responsibility of the computing community to focus on long term cybersecurity protocols. It is unrealistic to believe that we know where the future of cybersecurity may go seeing that technology is always evolving, but it is important that we study current trends to make informed predictions so that we may be able to better prepare ourselves for the future. This is why current cybersecurity techniques need to be taught throughout the computing community.

One of my favorite questions on cybersecurity was asked in "Cyber War: The Next Threat to National Security and What to Do about It" by Richard A. Clarke and Robert K. Knake. They posed the question:

"What do we do if we wake up one day and find the western half of the United States without electrical power as the result of a cyber-attack?"[34]

This question in particular put into perspective for me how important cybersecurity is by asking us what we could do to reverse an attack of this nature. With the entire western half of the U.S. without electrical power we would be relying on the eastern half of the U.S. to restore power. Even with today's technology, there is no telling how quickly this would be able to get done as an attack of this magnitude has never occurred within the United States. While the government would take control of the restoration process they would have to rely on help from the entire computing community. They would need computing individuals in the fields of networking, hardware, coding, and testing would also need to be included to assess the damage, check for remaining faults or added viruses, recoding of the system, and testing of the product before putting it back online. Even with a great number of people, without knowing how every electrical plant had their cybersecurity managed it would take a great deal of time to first find the

[34] Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What To Do About It*. Harper Collins. Print.

source of the attack and then even more time to try to correct the attack. As a country, however we do not have a publicly known plan of action for how the government would handle and attack like the one proposed.

While this whole idea is just a theory, with growing worldwide tensions and cyber warfare becoming a more commonly used attack method, it is critical that we start asking ourselves these types of questions because without a plan of action in place we have no idea how we would handle an attack of this nature. Because while it may only seem like an attack that would just involve electricity we sometimes fail to forget how much we rely on electricity for everyday actions such as pumping gas at the station or refrigeration. Within hours of this attack, we as a nation would see widespread panic, riots, and a crumbling economy, all of which would retain focus that could otherwise be used to remedy the attack. Therefore as other countries worldwide continue to focus more on education and technology, it is important we as a nation continue on the same path so that we keep a competitive advantage. This will not only help us develop as a nation, but it will also deter would be cyber-attacks.

At any moment an attack like this could happen and the only thing we can do is prepare ourselves for the moment. We need to make sure systems are secure and that we have a plan to rebuild after. However, by educating our current and future computing individuals now, we can help thwart off an attack of this nature. To begin with, I believe that cybersecurity techniques should be taught to anyone enrolled in a computer programming class. It is important that good coding techniques are taught from the early stages so that as programming skills are learned and developed so are good cybersecurity practices. This in the long term should result in safer code. Ideally it would also be encouraged for computer science programs to teach an introductory course in cybersecurity so that students could see if they are interested in pursuing the topic more and at the very least they will understand why cybersecurity is important.

For current computing individuals I believe it is important that they stay up to date on the latest threats and cybersecurity techniques. While there is no professional license necessary to code or skills that you must demonstrate before developing software, it is still important that individuals still continue to develop their skills through continuous learning. This can be done through workplace courses, local colleges/universities, or even through online training and information presentations. For example, information on emerging cybersecurity risks and protocols should be regularly included in IEEE or ACM publications which many computing professionals hold memberships in and receive information from.

For both current and future computing professionals it is important cybersecurity techniques are taught so that future technology is built to stand robustly against cyber-attacks. This may include making code harder to break into or making hardware less susceptible to physical attacks. It has also been noted that there is a current cybersecurity workforce crisis, which is another reason

why it is important to educate computing professionals about cybersecurity. In a report published in 2013 it was stated that the United States Cyber Command is currently seeking 5,000 cybersecurity pros while the federal government has a need for 10,000 cybersecurity experts and the Department of Homeland Security has an urgent need for 600 new cybersecurity employees.[35] By educating individuals now about cybersecurity, it would make it easier for individuals to be competitive for these jobs. Overall, it is important to the health of the computing profession for more individuals entering the field to have at least a basic background in cybersecurity, so that they can understand and appreciate the importance of it and know elementary ways in which to safeguard cybersecurity.

CONCLUSION

There is no doubt that as technology continues to get more advance that cybersecurity will become a greater issue. We have seen growing trends with cyber-attacks and they seem to continue to affect greater numbers of people each time. This was seen recently with the OpenSSL "Heartbleed" fault which left users vulnerable to attacks in which information like passwords, banking information, and healthcare data was threatened. An attacker through this fault could have stolen any of this information and left the system without leaving a trace.[36] While we still do not fully understand this most recent attack it may take years until we become fully aware of the outcome of the attack.

While the effects of "Heartbleed" is not fully known, there is no denying that cyber-attacks are continuing to grow and that everyone at some point in time will be a victim of one of these attacks. Even though we may not be able to predict or stop all attacks before they occur, hopefully by better preparing ourselves in the future we cannot only help identify and stop cyber-attacks, but through stronger and safer programming we may be able to slow down the rate in which attacks happen. Through education of our younger generations, we can begin the necessary steps to increase cybersecurity in our everyday lives and hopefully in the future generations to come they will be better equipped to handle cyber-attacks.

35 Corrin, Amber. "Is There a Cybersecurity Workforce Crisis?" *FCW*. The Business of Federal Technology, 15 Oct. 2013. Web.

36 "News Center." *MSN Money*. Reuters, 8 Apr. 2014. Web.

Works Cited

Adcox, Seanna. "S.C. Revenue Department Director: Agency Working to Restore Credibility." *The Post and Courier* [Charleston] 23 Apr. 2013. Web.

"Chronology of Data Breaches." *Privacy Rights Clearinghouse*. Web.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What To Do About It*. Harper Collins. Print.

Collier, Anne. "Cybersecurity Where Kids Are Concerned." *Connect Safely*. 1 Oct. 2013. Web.

Corrin, Amber. "Is There a Cybersecurity Workforce Crisis?" *FCW*. The Business of Federal Technology, 15 Oct. 2013. Web.

"Cyberbullying." *Kentucky.gov*. Office of the Attorney General, 2012. Web.

"Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." *U.S. GAO*. GAO, 14 Feb. 2013. Web.

Fryer-Biggs, Zachary. "Leadership Poll." *Defense News*. Defense News, 5 Jan. 2014. Web.

"News Center." *MSN Money*. Reuters, 8 Apr. 2014. Web.

"Public Sees U.S. Power Declining as Support for Global Engagement Slips." *Pew Research Center for the People and the Press RSS*. Pew Research, 3 Dec. 2013. Web.

Schiffner, Bill. "Could You Fall Victim to Crime Simply by Geotagging Location Info to Your Photos." *Digital Trends*. 22 July 2013. Web.

"School Children as Young as 11 to Get Cybersecurity Lessons." *Gov.uk*. 13 Mar. 2014. Web.

Shain, Andrew. "State Credentials Used to Access SC Taxpayer Data." The State, Oct. 2012. Web.

Sterling, Greg. "Pew: 94% Of Teenagers Use Facebook, Have 425 Facebook Friends, But Twitter & Instagram Adoption Way Up." *Marketing Land*. 21 May 2013. Web.

"Threat Terminology." *Network Experts*. Web.

"Top 10 Scams Targeting Seniors." *National Council on Aging*. Web. 2013.